

Cyber Jihad vs Cyberterrorism – Separating Hype from Reality

Dancho Danchev

Cybercrime Researcher, Security Blogger at ZDNet,
Security Blogger at Webroot Inc.



Who is Dancho Danchev?

- Internationally recognized cybercrime researcher
 - <http://ddanchev.blogspot.com>
- Security Blogger at CBS Interactive's ZDNet.com
 - <http://zdnet.com/blog/security>
- Security Blogger at Webroot Inc.
 - <http://blog.webroot.com>



What you will learn after this presentation?

- The difference between Cyber Jihad and Cyberterrorism
- The top 5 most popular Cyberterrorism myths
- Just how easy is it to become a Cyber Jihadist
- The current state of the Cyber Jihadist threat
- The hacking tools and tactics used by Cyber Jihadists to support their cyber operations



What you will learn after this presentation?

- Real life cases of Cyber Jihadist cyber operations in action
- Case study on the Global Islamic Media Front's (GIMF) cyber operations
- Are Cyber Jihadist's OPSEC (operational security) aware?
- The Intelligence Community's response



Presentation Outline

- Cyber Jihad VS Cyberterrorism – the basics
- Introduction to Cyber Jihad
- The current state of the Cyber Jihad threat
- The hacking tools and tactics used by Cyber Jihadists to support cyber operations
- Real life cases of Cyber Jihadists' cyber operations in action



Presentation Outline

- Case study on the Global Islamic Media Front's (GIMF) cyber operations



Cyber Jihad VS Cyberterrorism

- Introduction to Cyber Jihad
 - Propaganda/PSYOPS (psychological operations)
 - Potential target research
 - Fund raising
 - Recruitment/Radicalization/Training
 - 24/7/365 access to the Grid



Overview of Cyber Jihadists' Literature

- The Technical Mujahid Magazine
- Cyber Jihadist's Encyclopedia
- Mujahideen Harvest Magazine
- INSPIRE Magazine



Overview of Cyber Jihadists' Literature

- The Technical Mujahid Magazine
- Cyber Jihadist's Encyclopedia
- Mujahideen Harvest Magazine
- INSPIRE Magazine



The Technical Mujahid Magazine



3.3 ربط الدومين مع الاستضافة:

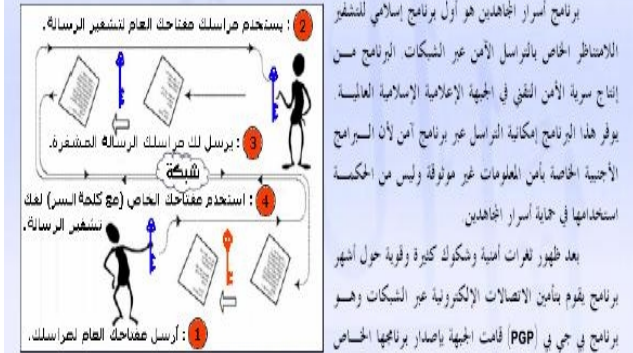
لربط الدومين مع الاستضافة يتوجب عليك العمل من ناحيتين: العمل من ناحية الدومين لإخباره بالسورفر اختوي على موقعك، والعمل في استضافتك لإخباره بموقعك.

في لوحة تحكم الدومين تجد خيار NS أو NS، في هذا الاختيار تستطيع تعديل اسم موقعك والذي هو غالباً يكون من عنوان أو أكثر بهذه الصورة NS1.host.com // NS2.host.com

المعنى	الدومين	المعنى	الدومين
تجاري	com	الإمارات	.ae
شبكة	.net	سوريا	.sy
المنظمات	.org	لبنان	.lf
معلومات (وهو من أخص النطاقات)	info	بريطانيا	.uk
منظمة أعمال	biz	إسرائيل	.il
موقع (Web Site)	.ws	السعودية	.sa
تلفزيون	.tv	العراق	.iq
شخصي	name	الأردن	.jo
تعليمي	.edu	مصر	.eg
حكومي	.gov	إيران	.ir

4. خلاصة:

في هذه المقالة تم شرح الخطوات الأساسية الأولى عندما نقرر إنشاء موقع جهادي على الانترنت. فبعد اختيار شركة الاستضافة وخطة الاستضافة والدومين يكون الموقع قد أنشئ، وفي الخطوات القادمة سنشرح كيف تتم إدارة الموقع وتزويد المواد عليه حتى ينتهي بنا المطاف بموقع جهادي متكامل إن شاء الله.



The Technical Mujahid Magazine

صاروخ أرض - جو قصير المدى تم تصميمه ليمنح القوات البرية طريقة فعالة للتعامل مع الطائرات والمروحيات التي تخنق على ارتفاع منخفض. من منظور الجهاد على الأرض فإن الطائرات المعادية التي تخنق على ارتفاع منخفض تشكل خطراً حقيقياً لأنها تكون إما في مهمة قصف، أو مراقبة، أو إنزال جود أو استخراجهم، أو إعادة تموين لقوات العدو (رسم 3-4). وإسقاط هذه الطائرات هي أسهل طريقة للقضاء على هذا الخطر.

خير مثال نذكره هو عمليات إسقاط 10 مروحيات في شهر واحد شملت جميع أنواع المروحيات مثل الأباتشي، بلاتك هوك، الشينوك، وحتى إسقاط طائرة من نوع إف-16 في منطقة الكوفة غرب بغداد، والعمليّة الأخيرة نفذها مجاهدو دولة العراق الإسلامية بالتعاون مع جيش المجاهدين وكان ذلك يوم الاثنين الموافق لـ 27/ 11/ 2006.



رسم 2 مجاهدو دولة العراق الإسلامية يطلقون صاروخ أرض- جو على مروحية شينوك في منطقة الكوفة. (لوني لفظ فحلت إطلاق الصاروخ على تمويل المروحة بن فيها من جود إلى كلفة من جيب. الصورة الوسطى بين الصاروخ الوجه قبل اصابتة بهدف. العمليّة بتاريخ 27/ 11/ 2007 نشرها مؤسسة الفرقان للإعلام)

تستخدم الصواريخ تستخدم مجسات حرارية أحادية اللون للأضعة تحت الحمراء تعمل في المجال 3-5 ميكرون للأطوال الإشعاع المنبعث من محرك الطائرة والناجم عن ثاني أكسيد الكربون (CO₂)، وهذا الإشعاع مُركّزٌ عند طول الموجة 4.2 ميكرون، كما أن هناك مجسات أحدث تشبه إلى حد كبير كاميرات حرارية تعمل في المجال 8-13 ميكرون مما يعطيها مقاومة عالية ضد الإجراءات المضادة، كما أن هذا المجال الترددي يقلل اعراضه من الجو وهذه المجسات تعرف ببنائية اللون. وأحدث مجسات مستخدمة هي $HgCdTe$ و $InSb$

من المميزات التي تجعل هذا النوع من الصواريخ سلاحاً فعالاً لاستخدام المجاهدين هي أن هذا السلاح خفيف ونقال، الصاروخ مع القاذبة يزنان ما بين 15 و 18 كجم، علماً أن القاذبة يعاد استخدامها والصاروخ وحده يزن ما بين 10 و 11 كجم شخص واحد يمكنه حمل القاذبة وإطلاق الصاروخ ليلاً أو نهاراً. هذا النوع من الصواريخ تنقل عليه عبارة "أطلق والنسج"، حيث أنه بعد إطلاق الصاروخ مباشرة يمكن الانسحاب من الموقع، ويقوم الصاروخ بتعقب الهدف تلقائياً عن طريق الحاسوب المدمج بداخله والذي يعتمد على نظام

الاتصالات السرية إخفاء الأسرار داخل الصور - بقلم أبي مصعب الجزائري

□ الاتصالات السرية: إخفاء الأسرار داخل الصور

بقلم: أبو مصعب الجزائري



أكثر شيء يخيف مكيب التحقيقات القدراتي الأمريكي هو استخدام المجاهدين لتقنيات الاتصالات السرية المعروفة بعلم الإخفاء

علم الإخفاء (Steganography) أو إخفاء المعلومات (Information Hiding) هو أحدث تقنية في النشل الآمن للمعلومات سواء كان ذلك عبر شبكة الانترنت، شبكة المخابرات النقال... أو غير ذلك من وسائل نقل المعلومات.

وبما يتل علم تشفير البيانات باستخدام خوارزمية القناع العام جماً لسرية المعلومة وأمن البيانات الخاصة، فسان نقطة الضعف في التشفير هو معرفة الآخر أنك تقوم بنقل معلومة مشفرة، وهذا في حد ذاته يشكل نوعاً من الخطر على مرسل البيانات المشفرة ويدفع الكثير من الأجهزة إلى متابعة الشخص المرسل نفسه ومعرفة مصدر الإرسال. وهنا يدخل علم إخفاء المعلومات، فهو يلغي نقطة ضعف علم التشفير بحيث يقوم بإخفاء المعلومات المشفرة بجميع أنواعها داخل بيانات أخرى مثل الصور والمقاطع الموسيقية أو غيرها. هذه الدراسة وطبقها التعريف بتقنية إخفاء المعلومات وتقنية كشف المعلومات الخفية - أو ما يعرف باسم "تحليل الإخفاء" -، كما سنحذر من عدد من البرامج التي تدعي إخفاءها للمعلومات بينما هي في حقيقتها برامج تخادعة لا يجب أن يستخدمها أحد لأن خسرها فادح، فحينما تعتد أنك قد أخفيت معلوماتك باستخدامك فإن استخراج هذه المعلومات يتم ببساطة شديدة علماً أن الصورة أعلاه توضيحية فقط وعمليّة الإخفاء تختلف جذرياً عما يظهر هنا.

رسائل السرية إخفاء الأسرار داخل الصور - بقلم أبي مصعب الجزائري

يجب أن تكون الاتصالات السرية

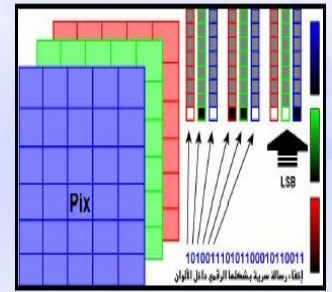
لـ كمية المعلومات المجهدة

ط طول الصورة (الحاملة للرسالة الخفية)

ع عرض الصورة

علماً أن هذه الكمية للمعلومات قبل إدخال الضغط عليها، فإذا تم استخدام ضغط المعلومات يعني أن الكمية سوف تكون أكبر بكثير مما حسبه. وهذا يعني مثلاً أنه من دون ضغط يمكنك إخفاء رسالة مكونة من 300 حرف في صورة بعرض 800 بكسل وارتفاع بكسل واحد. وعلى هذه الصورة لا يتم إخفاء أي شيء أصلاً في أي موقع للكرنل ويكون من ضمن تصميم لتوقع نفس ولا تثير أية شبهة طبعاً عند ضغط الرسالة يمكنك إخفاء كمية أكبر قد تصل إلى أضعاف الكمية التي قلنا مسبقاً.

و من البرامج المشهورة التي تقوم بدمج الرسائل أو المعلومات هذه الطريقة لذكر على سبيل المثال لا الحصر: EzStego, S-Tools, Hide and Seek لكن يجب أن نقر بين إخفاء المعلومات في صور لا نقتص للضغط والصور التي نضغط للضغط، حيث أن الضغط يقوم بتغير قيم الألوان حسب اختيار نوعية الصورة (image quality).



The Technical Mujahid Magazine



رسم 4. ميزات الملف الوسيط بين علامة نهاية الملف (EOF).

بعد استخدام برنامج الإخفاء (Steganography 1.8) فإننا نلاحظ أن البرنامج لم يدمج الملف الثاني داخل الملف الأول بل قام بالصاقه في نهاية الملف الأول (Concatenation).
بين الصورة التالية هذا الإخفاء حيث تظهر بيانات الملف الأول (الوسيط) باللون الأصفر ويظهر تحجها الملف الذي قام البرنامج بإخفائه. وفي الصورة التي تليها (رسم 7) تم إخفاء نفس الملف وحاجبه باستخدام كلمة سر. بمقارنة البيانات في الرسم 6 و الرسم 7 يتبين أن لا علاقة لكلمة السر بتشفير البيانات، فالبيانات في كلتا الصورتين متطابقة بغض النظر عن كلمة السر. وهذا يعني ببساطة أن البرنامج لا يقوم بتشفير البيانات اعتماداً على كلمة السر.



وُجدت العناوين الجانبية (Subtitles) من أجل إظهار ترجمة الأفلام بأي لغة دونما حاجة إلى التعامل مع برنامج تحرير الفيديو. وهي عبارة عن ملف صغير يحتوي على نص الترجمة ومعلومات المزامنة يوضع بجوار ملف الفيلم الأساسي ويحمل نفس اسمه مع اختلاف اللاحقة. فإذا قام المستخدم بتشغيل الفيلم يقوم برنامج التشغيل بإظهار نص الترجمة آلياً من الملف.

1. مراحل إنشاء العناوين الجانبية

عادةً فإن إنشاء العناوين الجانبية يمر بمرحلتين رئيسيتين:

- ♥ المرحلة الأولى: تحويل الكلام المنطوق في الفيلم إلى نص مكتوب باللغة المطلوبة.
- ♥ المرحلة الثانية: تقطيع هذا النص - تبعاً للسباق والمدة - إلى قطع صغيرة يتم مزامنتها مع محتوى الفيلم (أي ضبط توقيت بدء ظهور كل مقطع وتوقيت اختفائه).

رابط التبريل
<http://www.urusoft.net/downloads/subtitleworkshop251.zip>

تتم المرحلة الأولى وجزء التقطيع من المرحلة الثانية بشكل يدوي، أما مرحلة مزامنة المقاطع فيمكن لأجلها استخدام برنامج مساعد مثل: Subtitle Workshop.

1.1 طريقة مزامنة المقاطع باستخدام برنامج subtitle workshop

بعد فتح البرنامج عليك أن تنشئ ملف ترجمة جديد (من قائمة "ملف" اختر الأمر "ملف ترجمة جديد"). ثم عليك أن تحدد للبرنامج الفيلم الذي تريد العمل عليه (من قائمة "فيلم" اختر الأمر "فتح").

The Technical Mujahid Magazine

فن إخفاء الملفات



```
C:\fajr\hxdelf100r>cd \
C:\>net stop HackerDefender100
The service is not responding to the control function.
More help is available by typing NET HELPMSG 2186.

C:\>cd fajr
C:\fajr>cd hxdelf100r
C:\fajr\hxdelf100r>hxdelf100.exe :-uninstall
```

ملاحظات مهمة قبل البدء بعملية الرووت كت /

- (1) كما ذكرنا سابقاً من ملاحظة عدم تسمية العنوان الكامل للملف والاكتفاء باسم الملف فقط.
- (2) يجب إيقاف الإنترنت في جميع الفترة التي يكون فيها الرووت كت مفعلاً لأنه يحتوي على ما يسمى

لتسهيل فهم القياسات والاستفادة منها بصورة فعالة لعامة الناس؛ يتم إدخال خرائط جغرافية رقمية للجهاز بحيث يقوم الجهاز بإسقاط معلومات الموقع (جي بي إس) على الخارطة الرقمية ليظهر لك موقعك على الخارطة مباشرة. ونظام الخرائط الرقمية هنا اسمه نظام المعلومات الجغرافي. وفيما يلي المثال السابق مسقطاً على خارطة العراق.



صورة 7: دمج تحديد الموقع على خارطة جغرافية رقمية (جي بي إس - جي آي إس)

يبدو واضحاً أن تقاطع الدوائر هو النجمة الصفراء على الصورة. لكن هذه الدوائر هي تخيلية ولا تظهر على الجهاز.

Cyber Jihadist's Encyclopedia



Mujahideen Harvest Magazine



INSPIRE Magazine



Famous Cyber Jihadist Cases

- Irhabi007- caught and prosecuted
- Jihad Jane – caught and prosecuted
- GIMF members – caught and prosecuted



Cyber Jihadists' Hacking Teams

- Osama Bin Laden's Hacking Crew
- Ansar-AL-Jihad Hackers Team
- HaCKErS aL AnSaR
- The Designer – Islamic HaCKEr
- Alansar Fantom



STATUS: now absent from the *As. van derii* synonymy. See *W. J. H. H. H.* It has been lost but it does not of course fruit of course in this like as well as the other *Asch.*

Cyber Jihadists' Hacking Teams

The site
Hacked by

~¤ô§ô¤~

The Designer-Islamic HaCKEr

~¤ô§ô¤~

المصمم الاسلامي ~¤ô§ô¤~

~¤ô§ô¤~



Real life Cyber Jihadist Cyber Operations

- Al-Jinan's Electronic Jihad DoS Campaign
- Distribution of anti-infidel DIY Denial of Service Tools
- Muslims United Cyber DoS Campaign



Real life Cyber Jihadist Cyber Operations



Real life Cyber Jihadist Cyber Operations

free web hosting | free website | laptop computers | shopping cart | php hosting

There are a lot of ATMs out there.

Get a **FREE** Website [Click Here!](#)

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

أنصار الجهاد

بسم الله الرحمن الرحيم

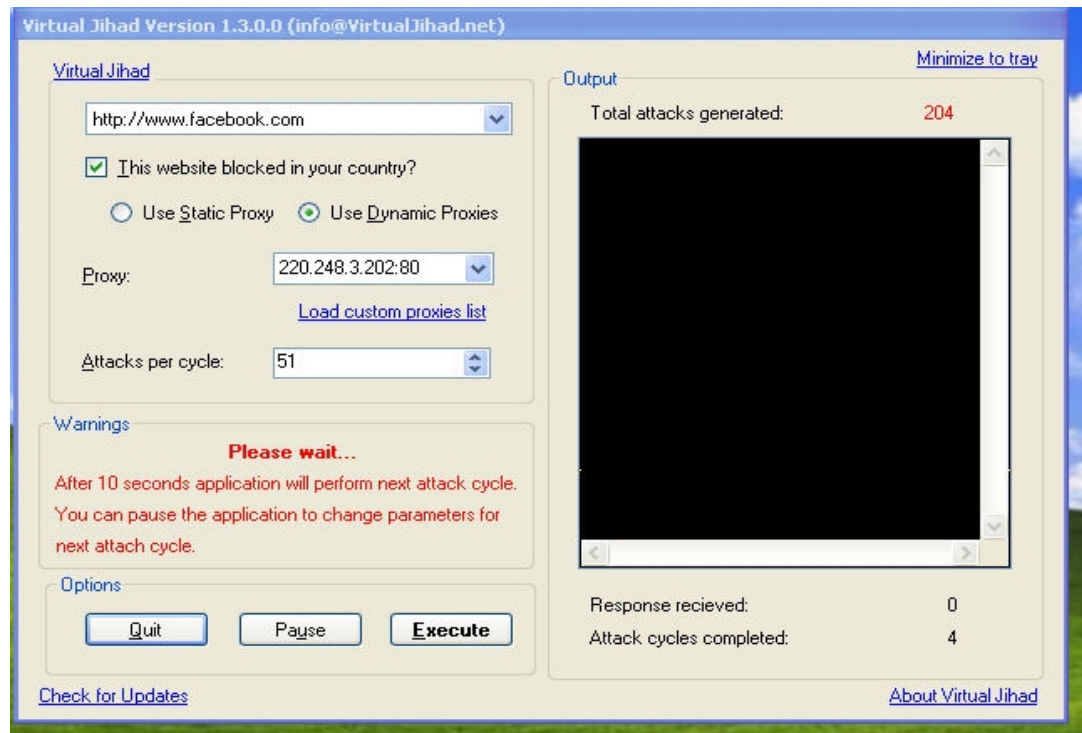
قال تعالى: (وما رميت اذ رميت ولكن الله رمى) صدق الله العظيم

هذه نتائج الهجمات التي قام بها المجاهدون في فريق أنصار الجهاد الالكتروني والتي وفقها الله بها بعصله

رقم الهجمة	الموقع	تصنيفه	استراتيجيتها	نتيجة الهجمة	حالة الآن
1	www.gov.il	موقع صهيوني كبير	الحاق أكبر الخسائر به	إيقافه لساعات عديدة بحمد الله	يعمل
2	www.keshmesh.net	موقع رافضي معادي لأهل السنة وكان ينشتم بالمجانين	إغلافه بإذن الله	تم إيقافه بالكامل والحاق خسائر كبيرة جدا به بحمد الله	ضعيف عاد بعد إغلافه أكثر من أربع شهور على...



Real life Cyber Jihadist Cyber Operations



Case study on GIMF

- First spotted in 2006 – released the “Night of Bush Capturing
- Releases the “Mujahideen Secrets Encryption Tool”
- Used primarily WordPress.com for hosting
- Relied on Archive.org for video hosting
- Abuse campaign to expose their social network



Case study on GIMF



Case study on GIMF




This blog has been archived or suspended for a violation of our [Terms of Service](#).

You can [create your own free blog on WordPress.com](#).

☺



Case study on GIMF




Web Moving Images Texts Audio Software Patron Info About IA Projects

Home Donate Forums FAQs Contributions Terms, Privacy, & Copyright Contact Volunteer Positions Jobs Bios


Search: creator:"Global Islamic Media Fr" All Media Types GO Advanced Search Anonymous User (login or join us)


Search Results

Results: 1 through 30 of 30 (0.005 secs)
You searched for: creator:"Global Islamic Media Front"





Global Islamic Media Front - الجبهة الإسلامية العالمية
تكم خطير و هام فلم ~ حتى لا يُختب المُنَادى~ شهادة الأخ أبي عبيد على جيش المجاهدين :: **Global Islamic Media Front** :: بسم الله الرحمن الرحيم ((الآن خُصَّصَ الحق)) الجبهة الإسلامية العالمية
Keywords: [الجبهة الإسلامية العالمية الآن خُصَّصَ الحق](#)
Downloads: 2,015






Global Islamic Media Front - قسم الإنتاج العربي : يقدم : [عشية استشهادية على مقر وزارة الثقافة والإعلام بكاابل]
Section of video production: report: [a martyrdom operation against the headquarters of the Ministry of Culture and Information in Kabul] The name of God the Merciful **Global Islamic Media Front** Department of Visual :: Submit:: [A martyrdom operation against the headquarters of the Ministry of Culture and Information in the puppet government] Cable This publication presents for the very movement of the Taliban, who claim that their illegal, and illustrates the extent of corruption, which is publi...
Keywords: [The war on Iraq, the Iraqi Islamic Party, the voice of Islam, Mujahideen, Jihad, and Zirstnan China, Pakistan, Taliban, Afghanistan](#)
Downloads: 1,125
Average rating: ☆☆☆☆☆ (0 review)





Jihad Hidden Camera : Bloody Comedy of American Soldiers in Iraq - Global Islamic Media Front
Jihad Hidden Camera : Bloody Comedy of American Soldiers in Iraq. A comedy made on the fighting styles of American soldiers in Iraq.
Keywords: [Jihad Hidden Camera : Bloody Comedy of American Soldiers in Iraq](#)
Downloads: 6,816
Average rating: ★★★★★ (9 reviews)



Case study on GIMF



Case study on GIMF

```
#---Begin GIMF ASRAR El Moujahedeen 1.0 Public Key 2048 bit---
pyHA5RbPuhWmwfeX+KjrJk9iHBjncI1sKN8CqTbYZR3K6nqk0hc1GXWnJ
U7QpiWlsqR6J+rsgSe8J5zJSh5oPCr2v2+K540q0MMwi8udJ5LpiWm20IoTy
ti0VrNxsXi0Mpohzc+pWOwMNDdaSKW11OyXc+kd3ybFRJHXNNUKpWDCn
/XPtSFNrWYj3vJVuBWh4VA7NTROdzW2uTMJcNo3IGQA/hYDAOWY6bm+GZ
qL+61gXzLv52gg9X8Fxe9vleG+sSt8sjThHGWO2W0WNGP5imvMG0ZtGaM
eVvmEKdTKQxCW3Wmib0I4qLjYxXCEg/JqQosrMPuXd4Jf4VTQLQB37Yk5Ny
91oBgAm+mbNJki9lko+mlAjD0MmjO+3niP/t19/Ezqb/+8EZvbrqmpBy2Jd
mm6CNTGX1PDLqGhPibTDnzL2WqghB7I34YX1ESXp/QXV7eKabdp6BkCqhw
8ZdDPcoLQzUbHswlRt8xcuSViHujCZ9Ds8OHhQqVizzXzCU1r1ApzWsiEu74cU
RAKcmqSbM2h1jGuSbastL/dUn/goxPGqTKjfvMq==
#---End GIMF ASRAR El Moujahedeen 1.0 Public Key 2048 bit---
```



Case study on GIMF



Case study on GIMF



Top 5 Most Popular Cyberterrorism Myths

- Cyberterrorists actively plot to take down the Grid
- Cyberterrorists exclusively use steganography
- Cyberterrorists poses sophisticated hacking skills
- Cyberterrorists use bullet-proof hosting services
- Cyberterrorists have access to good programmers with software engineering degrees



Thank you for your time and attention!

Dancho Danchev

Email: dancho.danchev@gmail.com

<http://ddanchev.blogspot.com>

<http://zdnet.com/blog/security>

<http://blog.webroot.com>

<http://twitter.com/danchodanchev>





Divider Slide Type

Section Title Here